



OSINT + ARCO + PROTECCIÓN DE DATOS

# MAPA-RD: Exposición y Ruta de Cierre

---

Así se ve tu entorno digital desde fuera. Esto es lo que hay que cerrar primero.

MAPA-RD identifica exposición real (visible públicamente), prioriza riesgos y entrega una ruta de cierre ejecutable. Incluye base operativa para gestión ARCO y un esquema mensual de control continuo.

Sin auditorías genéricas. Sin promesas vacías.

**ACME Corp · Reporte RPT-2026-001 · 2026-01-11**

Executive Security Report · Exposición pública · Confidencial

# Índice de Riesgo Digital

65

RIESGO CRÍTICO

# VECTORES DE VULNERABILIDAD

VEC-001	Exposed Database Credentials		85 <small>MÁXIMO</small>
ACTIVO: Production Database (AWS RDS)		TIPO: Cloud Infrastructure	EXPOSICIÓN: Public Repo Leak
<b>DESCRIPCIÓN DEL EVENTO</b>  Hardcoded credentials for the primary production database were identified in a public GitHub repository (config.js). Determining access logs confirmed unauthorized clone events.		<b>RUTA DE CIERRE</b>  <ol style="list-style-type: none"><li>Revoke the exposed AWS IAM credentials immediately.</li><li>Rotate the database master password.</li><li>Audit CloudTrail logs for suspicious activities since the commit date.</li><li>Implement git-secrets to prevent future commits.</li></ol>	
<b>IMPACTO</b> <ul style="list-style-type: none"><li>Full compromise of customer data (PII).</li><li>Potential total service disruption (Ransomware).</li><li>Severe regulatory fines (GDPR/CCPA).</li></ul>			

VEC-002

## Admin Portal without MFA

60 CRÍTICO

ACTIVO:  
admin.acme.com

TIPO:  
Web Application

EXPOSICIÓN:  
Missing Control

### DESCRIPCIÓN DEL EVENTO

The administrative panel allows single-factor authentication. Brute-force attacks or credential stuffing could easily compromise an admin account.

### IMPACTO

- Unauthorized administrative access.
- Data manipulation or deletion.
- Backdoor installation.

### RUTA DE CIERRE

- Enforce MFA (Time-based OTP) for all admin roles.
- Restrict access to VPN or trusted IPs only.
- Implement rate-limiting on the login endpoint.

VEC-003

## Outdated SSL Certificate

35 MEDIO

ACTIVO:  
dev.acme.com

TIPO:  
Dev Environment

EXPOSICIÓN:  
Configuration

### DESCRIPCIÓN DEL EVENTO

The SSL certificate for the development environment is expired, triggering browser warnings and exposing traffic to interception.

### IMPACTO

- Developer workflow disruption.
- Man-in-the-Middle (MitM) risk if used externally.
- Loss of trust validation.

### RUTA DE CIERRE

- Provision a new LetsEncrypt certificate.
- Automate renewal via Certbot.

# Anexo Técnico

METODOLOGÍA DE RIESGO V1.0 (OFICIAL)

## 1. Índice de Riesgo del Vector (IRV)

El **IRV** mide la urgencia y el impacto real de no remediar un vector de vulnerabilidad específico. Se calcula internamente mediante un modelo ponderado de seis dimensiones y se normaliza a una escala centesimal (0-100).

FÓRMULA GENERAL

$$IRV = [ \sum (Componente \times Peso) / \sum (Pesos\_Max) ] \times 100$$

### Variables del Modelo

#### CA (x4)

Criticidad del Activo. Evalúa la importancia del sistema afectado para la operación.

#### ET (x3)

Exposición Temporal. Determina si el hallazgo es histórico, residual o vigente.

#### SE (x3)

Superficie de Exposición. Mide la facilidad de acceso (Público vs Interno).

#### IM (x4)

Impacto Multidimensional. Suma binaria de impactos (Legal, Financiero, Operativo).

#### FE (x3)

Facilidad de Explotación. Nivel de esfuerzo técnico requerido por el atacante.

#### DV (x3)

Detectabilidad. Probabilidad de que el ataque pase desapercibido.

## 2. Índice de Riesgo Digital (IRD)

El **IRD** representa el estado global de riesgo de la organización. Es un indicador dinámico derivado exclusivamente de los IRV activos, utilizando un promedio ponderado por severidad.

CÁLCULO PONDERADO

$$IRD = \sum (IRV \times Peso\_Severidad) / \sum (Pesos\_Severidad)$$

ESCALA DE SEVERIDAD (PESOS)

BAJO	MEDIO	ALTO	CRÍTICO	MÁXIMO
Peso x1	Peso x2	Peso x3	Peso x4	Peso x5

Este documento es confidencial y parte integral del entregable MAPA-RD. La metodología v1.0 es propiedad intelectual cerrada.

Protegiendo la información que importa